UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DANIEL BORDEN, Individually, and on Behalf of All Others Similarly Situated,	)	Case No.
Plaintiff,	)	**JURY TRIAL DEMANDED**
v.	)	
DELOITTE CONSULTING, LLC	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Daniel Borden ("Plaintiff"), through his undersigned counsel, brings this action against Deloitte Consulting, LLC ("Deloitte" or "Defendant") pursuant to the investigation of his attorneys, personal knowledge as to himself and his own acts and otherwise upon information and belief, and alleges as follows:

INTRODUCTION

1. Deloitte Consulting, LLC ("Deloitte" or "Defendant") manages, maintains and operates the State of Rhode Island's RIBridges database, a database which maintains and manages state benefits, for Rhode Islanders, including health insurance, cash assistance, and child care benefits.[1]

[1] *See* https://www.providencejournal.com/story/news/local/2025/01/06/cyberattack-is-latest-bump-in-rhode-island-rocky-relationship-with-deloitte/77360234007/, last accessed January 16, 2025.

2. On or about December 23, 2024 news broke that a ransomware gang, now identified as "Brain Cipher"[2] accessed and leaked the sensitive personal information ("SPI") of approximately 650,000 Rhode Islanders whose SPI was part of the RIBridges database (the "Data Breach")[3].

3. It has been reported that this SPI includes at least names, addresses, dates of birth, Social Security numbers, and certain banking information.[4]

4. While the State of Rhode Island has announced that it began sending out notice letters on January 10, 2025[5], many (if not most) of the affected individuals have yet to receive letters. However, on information and belief, anyone who receives benefits through the RIBridges system has had their information stolen.[6]

5. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, including theft of their health insurance information.

---

[2] https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-in-rhode-islands-ribridges-breach/, last accessed January 16, 2025.

[3] *See* https://www.providencejournal.com/story/news/politics/2024/12/23/ri-cyberattack-could-expose-data-of-650000-people-what-to-know/77179680007/, last accessed January 16, 2025.

[4] *See* https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-in-rhode-islands-ribridges-breach/, last accessed January 16, 2025.

[5] *See* https://governor.ri.gov/press-releases/state-rhode-island-sends-official-letters-individuals-impacted-ribridges-data-breach, last accessed January 16, 2025.

[6] *See* https://admin.ri.gov/ribridges-alert, last accessed January 16, 2025.

6. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using your credit history;
- Making financial transactions on behalf of victims, including withdrawing monies from victims' accounts and opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

7. Plaintiff's and other Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of the Plaintiff and the other Class members.

8. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will remain for their respective lifetimes.

9. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's

conduct amounts to negligence and violates state statutes.

10. Plaintiff and similarly situated individuals, Class members, have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant's principal places of business is located within this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a

substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

14. Plaintiff Daniel Borden is a natural person and citizen of Rhode Island domiciled in Newport County, Rhode Island. Plaintiff has received benefits from RIBridges and his SPI has been stolen and exfiltrated as a result of the Data Breach.

15. Defendant Deloitte Consulting, LLC. is a for-profit Delaware corporation with its principal place of business at 30 Rockefeller Plaza, New York, New York. On information and belief, Defendant is a wholly-owned subsidiary of Deloitte Touche Tohmatsu Limited, a UK private company limited.

FACTUAL ALLEGATIONS

16. Defendant maintains the State of Rhode Island's benefits database.

17. This means that Defendant collects the SPI of individuals such as Plaintiff and the other Class members, including:

a. Contact and information, such as names, addresses, telephone numbers, email addresses, and household members;
b. Social Security numbers, and/or drivers license numbers; and
c. Banking information, including bank account and routing numbers;

d. Health insurance information, including account numbers and health histories; and

e. Additional information not yet determined.

18. On or about December 5, 2024, Defendant discovered that it had been the subject of a hack and exfiltration of the SPI of Rhode Islanders enrolled in the following programs:

- Medicaid
- Supplemental Nutrition Assistance Program (SNAP)
- Temporary Assistance for Needy Families (TANF)
- Child Care Assistance Program (CCAP)
- Health coverage purchased through HealthSource RI
- Rhode Island Works (RIW)
- Long-Term Services and Supports (LTSS)
- General Public Assistance (GPA) Program
- At HOME Cost Share[7]

19. On December 16, 2024, Defendant stated that the SPI stolen in the Data Breach likely included "names, addresses, dates of birth and Social Security numbers, and certain banking information."[8]

20. On December 31, 2024, a ransomware group known as Brain Cipher took credit for the hack and began leaking affected persons' SPI onto the dark web.[9]

---

[7] *See* https://www.bleepingcomputer.com/news/security/rhode-island-confirms-data-breach-after-brain-cipher-ransomware-attack/, last accessed January 16, 2025.

[8] *Id.*

[9] *See* https://www.healthcareitnews.com/news/brain-cipher-begins-leak-stolen-rhode-island-data, last accessed January 16, 2025.

21. While Rhode Island stated that notice letters began to be mailed on January 10, 2025, as of this writing, few people as have yet have received notice, and it is unknown if affected persons will be offered any recompense for the value of their lost SPI, time and money. On information and belief, anyone who receives benefits through the RIBridges system has had their information stolen.[10]

22. On December 30, 2024, *The Providence Journal* reported that the Governor's Office of Rhode Island had issued this statement: "[t]he state is working with Deloitte to generate the list of impacted individuals. Once we have that information, we will send letters to those individuals with instructions on how to access free credit monitoring"; and that "[w]e do not yet know the scope of the data that is included in those files, but as we've been saying for several weeks, we should assume that data contained in the RIBridges system has been compromised"[11]

23. However, this response has been entirely inadequate for Plaintiff and Class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

---

[10] *See* https://admin.ri.gov/ribridges-alert, last accessed January 16, 2025.

[11] *See* https://www.providencejournal.com/story/news/politics/2024/12/30/stolen-data-from-ri-hack-being-posted-to-the-dark-web-deloitte-confirms/77321958007/ , last accessed January 16, 2025.

24. Notably, this is not the Defendant's first problem in maintaining the RIBridges database. In 2017, it paid the State of Rhode Island $30 million to resolve allegations that it failed to properly establish and maintain the site.[12]

25. Further, it is not Defendant's first data breach. In 2017, it suffered a breach of its internal email system.[13]

26. Defendant had obligations created by contract, industry standards, common law, and public representations made to Plaintiff and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

27. Furthermore, at all relevant times, Defendant and/or its agents promulgated, adopted, and/or implemented in writing one or more Privacy Policies and HIPAA Notices in which it promised that Plaintiff's and other Class Members' SPI would be used and disclosed only under certain specific circumstances, none of which include or relate to those involved in the Data Breach.

28. On January 13, 2025 it was announced that individual notification letters had begun started to be mailed to the individuals whose personal data was stolen in the December 2024 ransomware attack on the RI Bridges system on January

---

[12] *See* https://rilawyersweekly.com/blog/2020/02/20/state-gets-30m-in-deloitte-settlement/, last accessed January 16, 2025

[13] *See* https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/, last accessed January 16, 2025.

10, 2025.[14] However, it was also reported that the data breach was "still being investigated by Deloitte and more individuals may have been affected than the initial review suggests. In such cases, notification letters will be promptly sent to those individuals."[15]

29. On February 5, 2025, it was reported that Deloitte had "agreed to pay $5 million to the state of Rhode Island to cover expenses incurred as a result of [the] December 2024 ransomware attack."[16] Globally, Deloitte reportedly generated $67.2 billion in fiscal year 2024, of which $33 billion was from the United States.[17]

30. A breakdown of the $5 million payment was reportedly not immediately available, but some of the money was supposedly to be used to cover "expenses incurred as a result of directly enrolling roughly 2,000 customers with Blue Cross & Blue Shield of Rhode Island and Neighborhood Health Plan of Rhode Island for the months of January and February, after the shutdown of HealthSource

---

[14] https://www.hipaajournal.com/rhode-island-ri-bridges-system-hack/ (last accessed February 5, 2025).

[15] https://www.hipaajournal.com/rhode-island-ri-bridges-system-hack/ (last accessed February 5, 2025).

[16] https://www.hipaajournal.com/rhode-island-ri-bridges-system-hack/ (last accessed February 5, 2025).

[17] https://rhodeislandcurrent.com/2025/02/04/deloitte-pays-5-million-to-rhode-island-to-cover-costs-of-ribridges-data-breach/ (last accessed February 5, 2025). *See also* https://www.deloitte.com/global/en/about/press-room/global-revenue-announcement.html (last accessed February 5, 2025) and

RI, the state's health insurance marketplace."[18]

31. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the healthcare industry preceding the date of the breach.

32. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to anyone in Defendant's industry, including Defendant.

33. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can significant take time, money, and patience to resolve.[19] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[20]

---

[18] https://rhodeislandcurrent.com/2025/02/04/deloitte-pays-5-million-to-rhode-island-to-cover-costs-of-ribridges-data-breach/

[19] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, last accessed January 16, 2025.

[20] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in

34. The SPI of Plaintiff and members of the Class was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the SPI for that purpose. The full scope and extent of the fraudulent activity resulting from the Data Breach may not come to light for years.

35. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and the Class, including dates of birth and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and other members of the Class a result of a breach.

36. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

37. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and other members of the Class.

---

conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

38. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

39. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.

40. The FTC guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

41. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party

service providers have implemented reasonable security measures.

42. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

43. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

44. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

45. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; securing protection against compromise communication systems; and

training staff regarding critical points.

46. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

47. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21]

48. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

49. General policy reasons support such an approach. A person whose

---

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, last accessed January 16, 2025.

personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

50. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

51. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The U. S. government and privacy experts acknowledge that it may take years for identity theft to come to

[22] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, last accessed January 16, 2025.

light and be detected.

52. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Class members, the former and current participants and/or applicants whose SPI was contained in RIBridges database and compromised in connection with the Data Breach, and whose Social Security numbers have been compromised, now face a real, present, imminent and substantial risk of identity theft and other material problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, in the latter case victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security

numbers are worth more than 10x on the black market."[23]

55. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the victim attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

56. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of SPI ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class members has materialized and is present and continuing, and Plaintiff and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their SPI; (e) invasion of privacy; and (f) the continued risk to their SPI, which remains in the

---

[23] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, last accessed January 16, 2025.

possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' SPI.

57. Plaintiff and Class members are at a heightened risk of identity theft for years to come.

58. The unencrypted SPI of Plaintiff and Class members may end up for sale on the dark web because that is the usual modus operandi of hackers. In addition, unencrypted SPI may fall into the hands of companies that will use the detailed SPI for targeted marketing without the approval of Plaintiff and Class members. Unauthorized individuals can easily access the SPI of Plaintiff and Class members.

59. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal SPI to monetize the stolen information. by selling it on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

60. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

61. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a his or her login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

62. One such example of criminals piecing together bits and pieces of compromised SPI for profit is the development of "Fullz" packages.[24]

63. With "Fullz" packages, cyber-criminals can cross-reference two sources of SPI to marry unregulated data available elsewhere to criminally stolen

---

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (one that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/, last visited January 16, 2025.

data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

64. The development of "Fullz" packages means here that the stolen SPI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the SPI that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

65. The existence and prevalence of "Fullz" packages means that the SPI stolen from the data breach can easily be linked to the unregulated data (like driver license numbers) of Plaintiff and the other Class members.

66. Thus, even if certain information (such as driver license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

67. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual learns that their SPI was compromised, the reasonable

person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

68. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions to try to remedy the harms they have experienced or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

69. These efforts are consistent with a U.S. Government Accountability Office report released in 2007 regarding data breaches that noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

70. These efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

[25] *See* GAO Report *supra* n.35.

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[26]

71. In addition, there can be substantial extra burden on particularly vulnerable segments of the population who are victims of such a data breach, such as those with physical or other disabilities who require but may have significant additional difficulty obtaining the substantial assistance to take the steps needed to protect themselves, their identities and their valuable information in the event.

72. And for those Class members who experience actual identity theft and fraud, the GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[27]

73. SPI is a valuable property right.[28] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts that include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that SPI has considerable market value.

74. Consequently, Plaintiff and Class members are at a present and

---

[26] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps, last accessed January 16, 2025.

[27] GAO Report *supra* n.35.

[28] *See, e.g.*, Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

continuous risk of fraud and identity theft for many years into the future.

75. The retail cost of credit monitoring and identity theft monitoring can be around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost that Plaintiff and Class members would not need to bear but for Defendant's failure to safeguard their SPI.

FACTS SPECIFIC TO PLAINTIFF

76. Plaintiff has used the services affected by the Data Breach in the past. Mr. Borden is a Rhode Island resident who is currently receiving benefits from the State of Rhode Island. Mr. Borden recently received a notice letter dated January 10, 2025 from the State of Rhode Island informing him that his "personal information was involved in a recent data breach." The letter described the breach as having been communicated to the State of Rhode Island on December 5, 2024 by Rhode Island vendor Deloitte, which informed it that "the RIBridges System may have been illegally accessed." The letter states that the breach was supposedly "confirmed" on December 10, 2024 and on December 11, 2024 it was confirmed that "personal information was compromised" affecting approximately 650,000 persons. A copy of the letter is annexed as Exhibit A.

77. The January 10, 2025 notice letter to Mr. Borden states that "[t]he information that may have been exposed includes names, addresses, dates of birth,

social security numbers, banking information, telephone number[s], and health information" and "[t]he type of information may vary for each individual and program."

78. Plaintiff has already spent more than ten hours dealing with the fallout from the breach, attempting to stay ahead of potential fraud related to the breach for example changing passwords on his credit card and other valuable or sensitive accounts.

79. Still, Plaintiff has experienced a drastic increase in spam texts recently, apparently as a result of this data breach, and has experienced the occurrence of incorrect information suddenly appearing on his credit report.

80. Prior to receiving the notice letter, Plaintiff took precautions after hearing about the breach and signed up for Experian credit monitoring service to also put a freeze on his credit, which will begin billing shortly at a monthly cost of $24.99.

81. Also, in early February, Plaintiff's bank account experienced an unauthorized access and fraudulent charge, apparently for a software company product that he did not request. He disputed the charge and it is reportedly currently being investigated by the bank.

82. Further, Plaintiff has experienced drastically increased anxiety, emotional distress, and increased concerns for the loss of his privacy and theft and

misuse of his valuable personal information since the time of the breach.

83. Plaintiff regularly takes steps to safeguard his own SPI in his own control. Plaintiff's time and efforts spent taking steps to protect his SPI have increased dramatically as a result of this disturbing data breach.

CLASS ACTION ALLEGATIONS

84. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All natural persons residing in the United States whose SPI was compromised in the Data Breach that was discovered in Defendant's systems on or about December 5, 2024.

85. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

86. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

87. **Numerosity**: The Class is so numerous that joinder of all members is impracticable. At this time, the number of class members is unknown, though new

estimates place the estimated number of class members around 650,000 persons.[29] The Class is readily identifiable within Defendant's records.

88. **Commonality**: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual members of the Class. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Class;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Class;

f. Whether Defendant knew or should have known that it did not

[29] *See* https://www.providencejournal.com/story/news/local/2025/01/06/cyberattack-is-latest-bump-in-rhode-island-rocky-relationship-with-deloitte/77360234007/, last accessed January 16, 2025

employ reasonable measures to keep the SPI of Plaintiff and members of the Class secure and to prevent loss or misuse of that SPI;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff and members of the Class damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Class that their SPI had been compromised; and

j. Whether Plaintiff and the other members of the Class are entitled to credit monitoring and other monetary relief.

89. **Typicality**: Plaintiff's claims are typical of those of the other members of the Class because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

90. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

91. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual member of the

Class are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

92. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

93. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendant failed to comply with their own policies and

applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(By Plaintiff Individually and on Behalf of the Class)

94. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 93.

95. Defendant routinely handles SPI that it acquires through various collection methods, such as Plaintiff's.

96. By collecting and storing the SPI of its customers, Defendant owed a duty of care to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

97. Defendant, as a subsidiary of one of the three major credit reporting agencies, is aware of that duty of care to the SPI of its customers.

98. Defendant has full knowledge of the sensitivity of the SPI and the types of harm that Plaintiff and Class Members could and would suffer if the SPI were

wrongfully disclosed.

99. Defendant knew or reasonably should have known that its failure to exercise due care in the collecting, storing, and using of their customers' SPI involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

100. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

101. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' SPI.

102. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

103. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the SPI of Plaintiff and the Class, the critical importance of providing adequate security of that SPI, and

the necessity for encrypting SPI stored on Defendant's systems.

104. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' SPI, including basic encryption techniques freely available to Defendant.

105. Plaintiff and the Class Members had no ability to protect their SPI that was in, and as far as they are aware, remains in, Defendant's possession.

106. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

107. Defendant had and continues to have a duty to adequately disclose that the SPI of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

108. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiff and Class Members.

109. Defendant has admitted that the SPI of Plaintiff and Class Members

was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

110. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiff and Class Members during the time the SPI was within Defendant's possession or control.

111. Defendant improperly and inadequately safeguarded the SPI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

112. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the SPI it had in its possession in the face of increased risk of theft.

113. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the SPI of Plaintiff and Class Members.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

115. But for Defendant's wrongful and negligent breach of duties owed to

Plaintiff and Class Members, the SPI of Plaintiff and Class Members would not have been compromised.

116. There is a close causal connection between Defendant's failure to implement security measures to protect the SPI of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' SPI was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to

undertake appropriate and adequate measures to protect the SPI of its employees and former employees in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as a result of the Data Breach for the remainder of Plaintiff's and Class Members' lives.

118. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Third-Party Beneficiary Contract
(By Plaintiff Individually and on Behalf of the Class)

119. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

120. Upon information and belief, Defendant entered into contracts with the State of Rhode Island to provide services to it; services that included data security practices, procedures, and protocols sufficient to safeguard the SPI that was entrusted to Defendant.

121. Such contracts were made expressly for the benefit of Plaintiff and the

Class, as it was their SPI that Defendant agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the SPI belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

122. Defendant knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

123. Defendant breached their contracts with the State of Rhode Island by, among other things, failing to adequately secure Plaintiff and other Class Members' SPI, and, as a result, Plaintiff and other Class Members were harmed by Defendant's failure to secure their SPI.

124. As a direct and proximate result of Defendant's breach, Plaintiff and other Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their SPI; (vii) future costs of

identity theft monitoring; (viii) and the continued risk to their SPI, which remains in Defendant's control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' SPI.

125. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

126. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant and/or its agents to, *e.g.*, (i) enhance data security measures, practices, systems and monitoring procedures; (ii) submit to future audits of those measures, practices, systems and monitoring procedures monitoring procedures on at least an annual basis; and (iii) immediately provide enhanced long term credit monitoring to all Class Members for a period of time significantly longer the one-year period previously offered in connection with the Data Breach, which is grossly insufficient.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract, in the Alternative
(By Plaintiff Individually and on Behalf of the Class)

127. Plaintiff re-alleges and incorporate by reference all of the allegations the paragraphs above 1 to 93.

128. Upon information and belief, Defendant committed to compliance with industry standards relating to data security, safeguards and protections, and to

ensure that Plaintiff's and other Class Members' SPI remained confidential and protected.

129. Further implicit in the agreement between Plaintiff and Class Members and the Defendant and/or its agent(s) to provide their SPI, was the latter's obligation to: (a) use such SPI for business purposes only, (b) take reasonable steps to safeguard that SPI, (c) prevent theft or unauthorized disclosures of the SPI, (d) provide Plaintiff and other Class Members with adequate and prompt notification of any and all instances unauthorized access and/or theft of their SPI, (e) reasonably safeguard and protect the SPI of plaintiffs and the other Class Members from theft and/or unauthorized disclosure or uses, (f) retain the SPI only under conditions that kept such information safe, secure and confidential and as long as necessary

130. The SPI of Plaintiff and the other Class Members was necessarily provided to Defendant and/or its agent(s) as a condition of their receiving services provided by Defendant and/or its third-party agents.

131. When the Plaintiff and the other Class Members provided their SPI to Defendant and/or its agent or agents as a condition of relationship(s) in which services were to be provided to the Plaintiff and the other Class Members, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such SPI.

132. Defendant required Class Members to provide their SPI to Defendant and/or its agents as part of regular business practices.

133. In entering into such implied contracts, Plaintiff and the other Class Members reasonably believed and expected that the data security practices of Defendant and/or its agent(s) would and did comply with pertinent, laws rules and regulations and with industry standards industry standards relating to data security, safeguards and protections.

134. The Plaintiff and other Class Members would not have entrusted their SPI to Defendant and/or its agents in the absence of the implied contract to keep their information reasonably safe, secure, confidential and free from unauthorized disclosure. The Plaintiff and the other Class Members would not have entrusted their SPI to Defendant and/or its agents in the absence of an implied promise to monitor the relevant computer systems and networks containing such SPI to ensure that reasonable data security measures had been implemented therein.

135. The Plaintiff and the other Class Members fully and adequately performed their obligations under the implied contracts with the Defendant.

136. The Defendant breached its implied contracts with the Plaintiff and the other Class Members by failing to adequately safeguard and protect their SPI.

137. As a direct and proximate result of the breaches of the implied contracts, the Plaintiff and other Class Members sustained damages as alleged herein.

138. Plaintiff and other Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

139. The Plaintiff and the other Class Members are also entitled to nominal damages for breach of implied contract.

140. The Plaintiff and the other Class Members are also entitled to injunctive relief requiring the Defendant and/or its agents to, e.g., (i) enhance data security measures, practices, systems and monitoring procedures; (ii) submit to future audits of those measures, practices, systems and monitoring procedures monitoring procedures on at least an annual basis; and (iii) immediately provide enhanced long term credit monitoring to all Class Members for a period of time significantly longer the one-year period previously offered in connection with the Data Breach, which is grossly insufficient.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiff Individually and on Behalf of the Class)

141. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs above 1 to 93.

142. Plaintiff and Class Members conferred a monetary benefit upon

Defendant when Defendant collected their SPI in such a way that profited Defendant.

143. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

144. The benefits given by Plaintiff and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

145. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

146. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

147. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein

FIFTH CLAIM FOR RELIEF
Declaratory Judgment
(By Plaintiff Individually and on Behalf of the Class)

148. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs above as if fully set forth herein.

149. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

150. Furthermore, the Court has broad authority to restrain conduct and acts, such as involved herein, that are tortious and violate the terms of federal and state laws as set forth herein.

151. The Defendant's Data Breach as described herein has resulted in an actual controversy concerning Defendant's present and prospective common law and other duties to reasonably safeguard and keep secure and confidential the Plaintiff's and other Class Members' SPI, and whether Defendant is currently maintaining data safety and security protection measures, protocols and systems that are sufficient to protect the SPI of the Plaintiff's and other Class Members from further data breaches in the future.

152. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer material injury as a result of the

unauthorized disclosure of their SPI and remain at significant and impending risk that further such compromises of their SPI will occur in the future.

153. Pursuant to this Court's authority under the Declaratory Judgment Act, it should enter judgment that, among other things:

a. Deloitte owed at all relevant times and continues to owe legal duties to secure, safeguard and keep confidential Class Members' SPI;

b. Deloitte owed at all relevant times and continues to owe legal duties to timely notify consumers of data breaches under the common law, under HIPAA, under Section 5 of the FTC Act, and/or under various other state laws, rules and/or regulations;

c. Deloitte has breached and continues to breach its legal duties by failing to employ data safety and security protection measures, protocols and systems that are sufficient to protect the SPI of the Plaintiff's and other Class Members from further data breaches in the future

d. provides for corresponding prospective injunctive relief requiring Defendant to employ such.

154. The risk of another such data breach by Deloitte is real, imminent, and significant, such that without such relief, the Plaintiff and other Class Members will suffer irreparable injury and lack sufficient legal remedy in the event of another such data breach by Defendant. If another breach at Deloitte occurs,

Plaintiff(s) and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

155. The hardships faced by the Plaintiff and other Class Members if such injunctive relief does not issue exceeds any hardship to Defendant by issuance of such an injunction because, among other things, if another such breach does take place, the Plaintiff and other Class Members will vulnerable to and likely be victims of fraud, identify theft, and other consequent harms described herein.

156. At the same time, Deloitte has pre-existing legal duties to implement and maintain reasonable and sufficient data safety and security protection measures, protocols and systems reasonable prospective data security measures, and the burden on Deloitte to comply with an injunction by instituting and implementing such measures is relatively minimal.

157. Nor will granting of such an injunction be in any way against the public interest, because such an injunction would if anything prevent another data breach at Deloitte, thus preventing additional resulting damages to Plaintiff and hundreds of thousands of others (at least) whose SPI is at risk of further compromise. Thus, issuance of such an injunction is would benefit the public and is in the public interest.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members,

requests judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' SPI;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying

information;

iv. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and

securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed

to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre- and post-judgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: February 7, 2025

Respectfully Submitted,
By: /s/ *Kent A. Bronson*

Kent A. Bronson
BRONSON LEGAL LLC
1216 Broadway (2nd Floor)
New York, NY 10001
Tel: (609) 255-1031
Fax: (609) 228-4997
bronsonlegalny@gmail.com

Carl V. Malmstrom*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

**Pro Hac Vice forthcoming*

Attorneys for Plaintiff and the Proposed Class

EXHIBIT A

STATE OF
RHODE ISLAND

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 10, 2025

[redacted]

[redacted]

DANIEL T BORDEN,

Your personal information was involved in a recent data breach. This letter tells you about the data breach and what you can do to protect your personal information. Please read this letter carefully. We understand this is a concerning situation, and we thank you for your patience.

What Happened: On December 5, 2024, the State was informed by its vendor, Deloitte, that information in the RIBridges system may have been illegally accessed. However, the State and Deloitte took steps right away to address the situation. Federal law enforcement, federal agencies and the Rhode Island State Police were notified. On December 10, 2024, it was confirmed that RIBridges was breached and, on December 11, 2024, that personal information was compromised. When and how the initial access happened are still being investigated. As of now, it is estimated that information of approximately 650,000 people may have been accessed.

What is RIBridges: RIBridges is a system that the State of Rhode Island uses to provide benefits, health insurance, and other programs to Rhode Islanders. RIBridges is maintained and operated by Deloitte for the State.

What Information was Involved in the Data Breach: The information that may have been exposed includes names, addresses, dates of birth, social security numbers, banking information, telephone number, and health information. The type of information may vary for each individual and program.

What We Are Doing for You

A Call Center Can Help Answer Questions

A call center in English, Spanish, and Portuguese can answer general questions about the breach and provide steps you can take now to protect yourself. The toll-free hotline is 833-918-6603. You can call Monday through Friday from 9 a.m. to 9 p.m. EDT and Saturday and Sunday from 11 a.m. to 8 p.m. EDT through January 19, 2025. After that date, the line will be open Monday through Friday from 9 a.m. to 9 p.m. EDT.

B137065, B137066

Free Credit Monitoring and Identify Theft Protection

Recipients of this letter can receive free credit monitoring and identity theft insurance for 5 years and identity restoration for your lifetime through Experian. The instructions to enroll are below. **Ensure that you enroll by April 30, 2025 (Your code will not work after this date.)**

For adults:

- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Use this **activation code**: ETPB548RWE
- If enrolling over the phone, be prepared to provide engagement number B137065

For children under 18 years old:

- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus
- Use this **activation code**: WQMG435RTX
- If enrolling over the phone, be prepared to provide engagement number B137066
- Provide your minor's information when prompted.

To enroll by phone as an adult or a child, please contact Experian's customer care team at 833-918-6603 by April 30, 2025 (5:59 UTC). Be prepared to provide the adult or child engagement number (above) as proof you should get free credit monitoring. You can also call that number if you have questions about the products or if you need help with identity restoration because of this breach.

What You Can Do

1. **Monitor Your Accounts** –We strongly encourage you to look out for signs of identity theft. Review your account statements, credit reports, and explanations of insurance benefits for unusual activity and to detect errors. Any charges or other activity that you do not recognize should be immediately reported to your insurance company, health care provider, and/or financial institution. Additionally:

   - **Change your passwords**; and
   - **Use multi-factor authentication**. This should require a one-time passcode via text message or email or an authenticator app in addition to password.

2. **Credit Freeze (also called Security Freeze)** – You can place a "credit freeze" (also called a "security freeze") on your credit report for free. **Credit freezes must be placed with each of the three credit bureaus: Equifax, Experian, and TransUnion.** Contact information for each of the credit bureaus are provided below.

   - A credit freeze restricts access to your credit report and helps **protect you from fraud**. When you place a credit freeze, creditors cannot access your credit report. This will prevent loans and any new credit from being approved in your name.
   - If you freeze your credit, **you will still be able to use your credit card**.
   - You can **lift the freeze at any time**.
   - To place a freeze by phone or mail, you may need to provide full name, Social Security number, date of birth, current address, and sometimes previous addresses, along with a copy of a government-issued ID like a driver's license. You can **learn more about credit freezes at the following website: www.usa.gov/credit-freeze**

3. **Identity Theft Reporting** – Please note that you have the right to file a police report if you ever experience identity theft or fraud, but you will likely need to provide proof that you have been a victim. Further, you may report instances of known or suspected identity theft to the **Rhode Island Office of the Attorney General, Consumer Protection Unit 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.**

4. **Free Credit Reports** – Additionally, under U.S. law, you are entitled to one free credit report once every 12 months from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

5. **Fraud Alerts** – You have the right to place an initial or extended "fraud alert" on a credit file for free for one year. If you place a fraud alert, a business is required to take steps to verify your identity before extending new credit. If you are the victim of identity theft, you can get an extended fraud alert for seven (7) years. You can contact any of the three major credit reporting bureaus listed below to place such fraud alerts. **If you ask one credit bureau to place a fraud alert on your file, they will report it to the remaining two credit bureaus for you.**

6. **Further Information** – Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by using the contact information listed above.

You may also visit cyberalert.ri.gov for more updates on the data breach and information on protecting yourself.

Credit Freeze and Fraud Alert Contact Information – Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Credit Bureau	Equifax	Experian	TransUnion
Online	www.equifax.com/personal/credit-report-services	www.experian.com/help/	www.transunion.com/customer-support/
By Phone	1-888-298-0045	1-888-397-3742	1-800-916-8800
By Mail: Fraud Alert (alerting one alerts them all)	Equifax Fraud Alert, P.O. Box 105069, Atlanta GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen TX, 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
By Mail: Credit Freeze (each bureau must be alerted individually)	Equifax Credit Freeze Alert, P.O. Box 105788, Atlanta GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen TX, 75013	TransUnion Credit Freeze, P.O. Box 160, Chester, PA 19094

ATTENTION: Language assistance services are available to you free of charge. Call . 1-855-697-4347 (TTY 711).

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-855-697-4347 (TTY 711)

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-855-697-4347 (TTY 711)

注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-855-697-4347 (TTY 711)

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-855-697-4347 (TTY 711)

ប្រយ័ត្ន៖ បើសិនជាអ្នកនិយាយ ភាសាខ្មែរ, សេវាជំនួយផ្នែកភាសា ដោយមិនគិតឈ្នួល គឺអាចមានសំរាប់បំរើអ្នក។ ចូរទូរស័ព្ទ 1-855-697-4347 (TTY 711)

ATTENTION: Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-855-697-4347 (ATS 711)

ATTENZIONE: In caso la lingua parlata sia l'italiano, sono disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 1-855-697-4347 (TTY 711)

ໂປດຊາບ: ຖ້າວ່າ ທ່ານເວົ້າພາສາ ລາວ, ການບໍລິການຊ່ວຍເຫຼືອດ້ານພາສາ, ໂດຍບໍ່ເສັງຄ່າ, ແມ່ນມີພ້ອມໃຫ້ທ່ານ. ໂທຣ 1-855-697-4347 (TTY 711)

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم (رقم هاتف الصم والبكم: 1-855-697-4347 TTY 711

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 1-855-697-4347 (телетайп 711)

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 1-855-697-4347 (TTY 711)

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 1-855-697-4347 (TTY 711)

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-855-697-4347 **(TTY 711)** 번으로 전화해 주십시오

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 1-855-697-4347 (TTY 711).

Dè dɛ nìà kɛ dyédé gbo: Ɔ jû ké m̀ [Bàsɔ́ɔ́-wùdù-po-nyɔ̀] jû ní, níí, à wudu kà kò dò po-poò bɛ́ín m̀ gbo kpáa. Đá 1-855-697-4347 (TTY 711)

Non-Discrimination Notice
The Executive Office of Health and Human Services (EOHHS) and the Department of Human Services (DHS) does not discriminate on the basis of race, color, national origin, disability, political beliefs, age, religion or gender in acceptance for or provision of services, employment or treatment, in its education and other program activities. Under other provisions of applicable law, EOHHS/DHS does not discriminate on the basis of sexual orientation, gender identity or expression. For further information about these non-discrimination laws, regulations and complaint procedures for resolution of complaints of discrimination, contact DHS at 25 Howard Ave, Bldg. 57, Cranston, RI 02920, telephone number (401) 462-2971 (for deaf/hearing impaired 1-800-745-6575 voice; TTY 711).